



UNIVERSITY OF MARY WASHINGTON

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2018

Auditor of Public Accounts
Martha S. Mavredes, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

We have audited the basic financial statements of the University of Mary Washington as of and for the year ended June 30, 2018, and issued our report thereon, dated April 3, 2019. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.umw.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance or other matters required to be reported under Government Auditing Standards.

–TABLE OF CONTENTS–

Pages

AUDIT SUMMARY

STATUS OF PRIOR YEAR AUDIT FINDINGS

1

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

2-3

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER
FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

4-6

UNIVERSITY RESPONSE

7-8

UNIVERSITY OFFICIALS

9

STATUS OF PRIOR YEAR AUDIT FINDINGS

Conduct Information Technology Security Audits on Sensitive Systems

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2017)

The University of Mary Washington (University) is not performing timely information technology (IT) security audits on its sensitive IT systems in accordance with the Commonwealth's IT Security Audit Standard, SEC 502 (IT Audit Standard). The University's adopted information security standard, which is the Commonwealth's Information Security Standard, SEC 501 (Security Standard), requires IT security audits for sensitive systems in accordance with the IT Audit Standard. The University *Internal Audit Charter* tasks the Internal Audit department with performing IT security audits. However, the University does not conduct a comprehensive IT security audit on each sensitive system at least once every three years that assesses whether IT security controls implemented to mitigate risks are adequate and effective.

The Security Standard, Section 7, requires that each IT system classified as sensitive undergo an IT security audit as required by and in accordance with the current version of the IT Audit Standard. The IT Audit Standard, Section 1.4, requires that IT systems containing sensitive data, or systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall receive an IT security audit at least once every three years. Additionally, the IT Audit Standard, Section 2.2, requires that the IT Security auditor shall use criteria that, at a minimum, assess the effectiveness of the system controls and measure compliance with the applicable requirements of the Security Standard.

Without conducting full IT security audits that cover all applicable Security Standard requirements for each sensitive system, the University increases the risk that IT staff will not detect and mitigate existing weaknesses in sensitive systems. Malicious parties taking advantage of continued weaknesses could compromise sensitive and confidential data. Further, such security incidents could lead to mission critical systems being unavailable.

The Internal Audit department developed a fiscal year 2019 audit plan, but did not conduct any of the planned audits, due to turnover within the Internal Audit department. The University hired a new Director of Internal Audit in January 2019. The Internal Audit department plans to obtain approval for a three-year audit plan by March 2019. Subsequently, the University plans to begin a rotating audit schedule to include an audit of each sensitive system within three years, beginning in fiscal year 2020.

Management should evaluate potential options and develop a formal process for conducting IT audits over each sensitive system at least once every three years that tests the effectiveness of the IT security controls and compliance with Security Standard requirements. Compliance with the IT Audit Standard will help to ensure the confidentiality, integrity, and availability of sensitive and mission critical data.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Security Awareness Training

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

The University is not meeting certain requirements in the Security Standard, for security awareness training. An established security awareness training program is essential to protecting agency IT systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information at the University. Our review of the University's security awareness training program identified the following weaknesses:

- The University does not monitor completion of security awareness training for all employees and contractors and enforce compliance with the annual security awareness training requirement. The University transitioned to using a new training program, and established and documented procedures governing the new process; however, the University has not yet enforced compliance using the new process during a training cycle. The Security Standard requires security awareness training for all information system users, including contractors, initially upon employment, after significant changes in the environment, and annually thereafter. Without implementing a process to ensure all users take security awareness training annually, the University increases the risk that untrained users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering. (*Security Standard section: AT-2 Security Awareness*)
- The University does not require and provide applicable role-based security training to all personnel with assigned security roles and responsibilities. The University provides role-based security training to IT staff, but does not require or provide role-based security training to management and operational staff with assigned security roles and responsibilities (e.g., System Owner and Data Owner). Additionally, the University does not require or provide role-based security training to contractors providing services to the University. The Security Standard requires that the University provide role-based security training before granting access to the system, after significant changes in the environment, and as practical and necessary thereafter. Lack of adequate role-based security training increases the risk that users will be unaware or unequipped to perform their assigned security related functions, resulting in an increased data security risk. (*Security Standard section: AT-3 Role-Based Security Training*)

The time required to define and establish a workable solution to enforce users' completion of annual security training delayed the University's transition to its new security awareness training procedure and process. Additionally, the University has been without an information security officer since fall 2018, which delayed completion of the project.

The University should implement its documented procedure to monitor and enforce completion of annual security awareness training. Additionally, the University should require all employees and contractors with assigned security roles to complete applicable role-based training. Improving the security awareness training program will help protect the University from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

Comply with Federal Regulations for Documentation of Employment Eligibility

Type: Compliance

Severity: Not Applicable

Repeat: No

The University does not properly complete Employment Eligibility Verification (I-9) forms for some new employees. For two of eleven employees (18 percent) tested, University personnel did not sign the I-9 form within three days of the employee's date of employment. For one of eleven employees (9 percent), University Human Resources (HR) personnel did not ensure proper completion of Section 1 and Section 3 (returning employee) of the form until fifteen days after the employee's start date.

The Immigration Reform and Control Act of 1986, requires that employers complete an I-9 form to verify both identity and employment eligibility for all employees hired after November 6, 1986. Additionally, the U.S. Department of Homeland Security's Guidance for Completing Form I-9 Handbook for Employers issued by the U.S. Citizenship and Immigration Services prescribes federal requirements for completing I-9 forms. Not complying with federal requirements could result in civil and/or criminal penalties and debarment from government contracts.

Human Resources indicated that the form completed and signed late related to a returning student employee and that Student Employment in the Office of Financial Aid did not communicate with HR to ensure proper completion of all employment paperwork. For the unsigned form, HR back-dated and signed the form to agree to the e-Verify confirmation date and returned it to the auditor, which does not comply with the established federal procedures for updating improperly completed I-9 forms.

Human Resources should communicate I-9 requirements and provide adequate training and resources to hiring managers to reinforce the expectation to comply with the applicable federal requirements. In addition, HR should perform an adequate review of I-9 forms completed by hiring managers.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

April 3, 2019

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
University of Mary Washington

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component unit of the University of Mary Washington as of and for the year ended June 30, 2018, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated April 3, 2019. Our report includes a reference to another auditor. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component unit of the University, which were audited by another auditor in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. We did identify certain deficiencies in internal control over financial reporting entitled "Conduct Information Technology Security Audits on Sensitive Systems" and "Improve Security Awareness Training," which are described in the sections titled "Status of Prior Year Audit Findings" and "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the sections titled "Status of Prior Year Audit Findings" and "Internal Control and Compliance Findings and Recommendations" in the findings entitled "Conduct Information Technology Security Audits on Sensitive Systems," "Improve Security Awareness Training," and "Comply with Federal Regulations for Documentation of Employment Eligibility."

The University's Response to Findings

We discussed this report with management at an exit conference held on April 4, 2019. The University's response to the findings identified in our audit is described in the accompanying section titled "University Response." The University's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

The University has not taken adequate corrective action with respect to the previously reported finding “Conduct Information Technology Security Audits on Sensitive Systems.” Accordingly, we included this finding in the section entitled “Status of Prior Year Audit Findings.” The University has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity’s internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Audit Standards in considering the entity’s internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

AUDITOR OF PUBLIC ACCOUNTS

EMS/vks

April 4, 2019

Ms. Martha Mavredes
Auditor of Public Accounts
P O Box 1295
Richmond, Virginia 23218

Subject: Management response to the Audit Recommendations for Fiscal Year 2018

Dear Ms. Mavredes,

I am pleased to send you University of Mary Washington's response to the internal control findings and recommendations identified during the audit of the fiscal year ended June 30, 2018. Management's responses are as follows.

Conduct Information Technology Security Audits on Sensitive Systems

Audit of two sensitive systems has been included in the University's fiscal year 2020 audit plan. Management has also committed to complete audits of all sensitive systems over the next three fiscal years, and to maintain compliance with the audit requirement thereafter. The fiscal 2020 audit plan will be completed by June 30, 2020.

Improve Security Awareness Training

The University's Information Technology Department will implement processes and controls to enforce compliance with the annual security awareness training requirement, as well as expand role-based training based on employee/contractor role or job function. Implementation of this process will be complete by December 31, 2019.

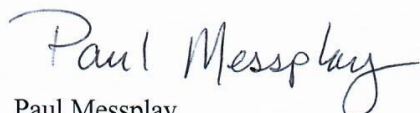
Comply with Federal Regulations for Documentation of Employment Eligibility

Management will provide additional training to appropriate staff to ensure proper completion, review and correction of I-9 forms. Human Resources will work with Student Employment to ensure awareness of Federal Requirements for I-9 documentation. In addition, Human Resources will conduct an internal audit of all I-9 forms. The University expects completion of this training and review by December 31, 2019.

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu

If you have any questions or need additional information, please do not hesitate to contact me by phone at (540) 654-1410 or by email at pmesspla@umw.edu

Sincerely,



Paul Messplay
Vice President for Administration and Finance

1301 College Avenue
Fredericksburg, VA 22401-5300
www.umw.edu

UNIVERSITY OF MARY WASHINGTON

As of June 30, 2018

BOARD OF VISITORS

Fred M. Rankin, III, Rector
Kenneth J. Lopez, Vice Rector
Heather M. Crislip, Secretary

Sharon Bulova	R. Edward Houck
Holly T. Cuellar	Davis C. Rennolds
Carlos Del Toro	Lisa D. Taylor
Edward B. Hontz	Rhonda S. VanLowe
Deirdre Powell White	

ADMINISTRATIVE OFFICERS

As of March 31, 2019

Troy D. Paino
President

Paul Messplay
Vice President for Administration and Finance

Julie Smith
Associate Vice President for Finance

Davis McCrory
Director of Internal Audit